

特開平5-244150

(43) 公開日 平成5年(1993)9月21日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
G 0 9 C 1/00		9194-5L	H 0 4 L 9/00	Z
		7117-5K		
			審査請求 未請求 請求項の数17(全 22 頁)	

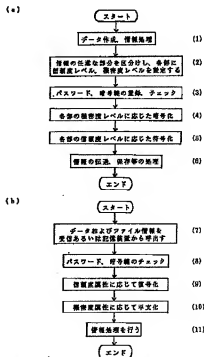
(21) 出願番号	特願平3-215909	(71) 出願人	591059384 岡野 博一 広島県広島市安佐北区倉掛1丁目8-6
(22) 出願日	平成3年(1991)7月31日	(72) 発明者	岡野 博一 広島県広島市安佐北区倉掛1丁目8-6
(31) 優先権主張番号	特願平2-204337		
(32) 優先日	平2(1990)7月31日		
(33) 優先権主張国	日本 (J P)		
(31) 優先権主張番号	特願平2-243004		
(32) 優先日	平2(1990)9月12日		
(33) 優先権主張国	日本 (J P)		
(31) 優先権主張番号	特願平3-61295		
(32) 優先日	平3(1991)3月1日		
(33) 優先権主張国	日本 (J P)		

(54) 【発明の名称】 知的情報処理方法および装置

(57) 【要約】

【目的】 本発明の目的は、文書、図形、画像、データベース等の情報伝送および処理に於て、情報各部の属性に応じて、効率的な誤り訂正符号と暗号化技術を適用し、ついで、情報各部分を機密度レベルに応じて暗号化し、そのアクセスを複数の特定者に限定する。さらに暗号文のファイル管理を容易にし、柔軟な電子文書システム、ファイル管理システムの構築に有効なセキュリティ機能を有する知的情報処理方法および装置を提供することである。

【構成】 情報処理システムに、誤り訂正符号の機能、暗号化機能を付加する。



1

【特許請求の範囲】

【請求項1】 文書、図形、画像等の情報伝送および処理において、信頼度レベルとして0からmまでのレベルを用い、また、機密度レベルとして0からnまでのレベルを用いて、CRT等の表示部上で、情報の任意の各部分に、信頼度レベルと機密度レベルの属性を設定し、それぞれに応じた誤り訂正符号と暗号化の技法および暗号鍵を用いて、符号化および暗号化を行い、情報処理および伝送、保存を行う、下記の(1)ないし(6)の手順と、符号化および暗号化されたデータを受信あるいは外部メモリから呼び出し、復号化および平文化を行い情報の処理を行う、下記の(7)ないし(11)の手順とを含むことを特徴とする知的情報処理方法。

- (1)文書、図形、画像等のデータを作成する手順。
- (2)情報の任意の部分区分けし、その情報各部に信頼度レベルと機密度レベルの属性を設定する手順。
- (3)パスワード、暗号鍵のチェックを行う手順。
- (4)情報各部をその機密度レベルに応じた暗号化法あるいは暗号鍵を用いて暗号化する手順。
- (5)情報各部をその信頼度レベルに応じた誤り訂正符号を用いて符号化する手順。
- (6)符号化および暗号化された情報を、伝送あるいは保存等の処理を行う手順。(7)データ、ファイルを受信あるいは外部メモリから呼び出す手順。
- (8)パスワード、暗号鍵のチェックを行う手順。
- (9)信頼度属性に応じて情報各部を復号化する手順。
- (10)機密度属性に応じて情報各部を平文化する手順。
- (11)情報処理を行う手順。

【請求項2】 請求項1記載の知的情報処理方法において、情報属性として機密度レベルのみを使用し、そのレベルとして0からnまでのレベルを用いて(レベル0、1のみを使用する方法を含む)、CRT等の表示部上で、情報の任意の部分区分けする手順と、その情報各部に、機密度レベルの属性を設定する手順と、それぞれに応じた暗号化の技法および暗号鍵を用いて暗号化および平文化を行う手順とを含むことを特徴とする知的情報処理方法。

【請求項3】 請求項1記載の知的情報処理方法において、情報属性として信頼度レベルのみを使用し、そのレベルとして0からmまでのレベルを用いて(レベル0、1のみを使用する方法を含む)、CRT等の表示部上で、情報の任意の部分区分けする手順と、その情報各部に、信頼度レベルの属性を設定する手順と、それぞれに応じた誤り訂正符号を用いて符号化および復号化を行う手順とを含むことを特徴とする知的情報処理方法。

【請求項4】 文書、図形、画像等の情報伝送および処理において、信頼度レベルとして0からmまでのレベルを用い、また、機密度レベルとして0からnまでのレベルを用いて、CRT等の表示部上で、情報の任意の各部分に、信頼度レベルと機密度レベルの属性を設定し、そ

2

れぞれに応じた誤り訂正符号と暗号化の技法および暗号鍵を用いて、符号化および暗号化を行い、情報処理および伝送、保存を行う、下記の(1)ないし(6)の手段と、符号化および暗号化されたデータを受信あるいは外部メモリから呼び出し、復号化および平文化を行い情報の処理を行う、下記の(7)ないし(11)の手段とを含むことを特徴とする知的情報処理装置。

- (1)文書、図形、画像等のデータを作成する手段。
- (2)情報の任意の部分区分けし、その情報各部に信頼度レベルと機密度レベルの属性を設定する手段。
- (3)パスワード、暗号鍵のチェックを行う手段。
- (4)情報各部をその機密度レベルに応じた暗号化法あるいは暗号鍵を用いて暗号化する手段。
- (5)情報各部をその信頼度レベルに応じた誤り訂正符号を用いて符号化する手段。
- (6)符号化および暗号化された情報を、伝送あるいは保存等の処理を行う手段。(7)データ、ファイルを受信あるいは外部メモリから呼び出す手段。
- (8)パスワード、暗号鍵のチェックを行う手段。
- (9)信頼度属性に応じて情報各部を復号化する手段。
- (10)機密度属性に応じて情報各部を平文化する手段。
- (11)情報処理を行う手段。

【請求項5】 請求項4記載の知的情報処理装置において、情報属性として機密度レベルのみを使用し、そのレベルとして0からnまでのレベルを用いて(レベル0、1のみを使用する方法を含む)、CRT等の表示部上で、情報の任意の部分区分けする手段と、その情報各部に、機密度レベルの属性を設定する手段と、それぞれに応じた暗号化の技法および暗号鍵を用いて暗号化および平文化を行う手段とを含むことを特徴とする知的情報処理装置。

【請求項6】 請求項4記載の知的情報処理装置において、情報属性として信頼度レベルのみを使用し、そのレベルとして0からmまでのレベルを用いて(レベル0、1のみを使用する方法を含む)、CRT等の表示部上で、情報の任意の部分区分けする手段と、その情報各部に、信頼度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号を用いて符号化および復号化を行う手段とを含むことを特徴とする知的情報処理装置。

【請求項7】 機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだまま、平文部分の見出し、キーワード等のファイル管理に必要な情報を直接操作あるいは検索してファイル管理を行う手段とを含むことを特徴とする知的情報処理方法。

【請求項8】 機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだまま、平文部

3

分の見出し、キーワード等のファイル管理に必要な情報を直接操作あるいは検索してファイル管理を行う手段とを含むことを特徴とする知的情報処理装置。

【請求項9】 データベース・システムの任意の、データ項目、レコード（行情報）、データ項目全体（列情報）にその信頼度レベルおよび/または機密度レベルの属性を設定する手順と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手順とを含むことを特徴とする請求項1記載の知的情報処理方法。

【請求項10】 データベース・システムの任意の、データ項目、レコード（行情報）、データ項目全体（列情報）にその信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手段とを含むことを特徴とする請求項4記載の知的情報処理装置。

【請求項11】 データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分とを区分けする手段と、その各部分に、信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手段とを含むことを特徴とする請求項1記載の知的情報処理方法。

【請求項12】 データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分とを区分けする手段と、その各部分に、信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手段とを含むことを特徴とする請求項4記載の知的情報処理装置。

【請求項13】 文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0からnまでのレベル（レベル0、1のみを使用する方法を含む）を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにあってはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定し、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化を行う情報処理において、機密度レベルに対応させてアクセス権限レベルを設定し、パスワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する手順を含むことを特徴とする知的情報処理方法。

【請求項14】 文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0か

4

らnまでのレベル（レベル0、1のみを使用する方法を含む）を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにあってはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定し、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化を行う情報処理において、機密度レベルに対応させてアクセス権限レベルを設定し、パスワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する手段を含むことを特徴とする知的情報処理装置。

【請求項15】 機密を要するファイルおよびデータを回線暗号化して伝送する際、ファイル管理、暗号化処理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだファイル、データを、さらに、回線暗号化する手段と、それを伝送する手段とを含むことを特徴とする知的情報処理装置。

【請求項16】 ファクシミリを用いて、文書を伝送する際、送信文書にシール添付領域を設けバーコード等のシールをはるか、行カウント機能を利用する等して、行単位あるいはドット単位等に同一ページ内の通常文と機密を要する文を区分する手段と、通常文は普通に伝送し、機密を要する文は暗号化機能に切替えて暗号化して伝送する手段と、受信側では、いったん暗号文を含んだ全文を記憶装置に格納するとともに、通常文のみ印刷出力した後、パスワード、暗号鍵を利用して暗号文の平文化、印刷などの処理を特定者のみに限定する手段とを含むことを特徴とする請求項4記載の知的情報処理装置。

【請求項17】 使用する装置あるいはソフトウェアなどに使用する暗号鍵を登録し、その履歴リストを作成しておき、場合によっては暗号化して保存し、暗号鍵の忘却、紛失の際、その履歴リストを利用して、ファイルあるいはその部分に対して使用した暗号鍵を検索、検証して検し出す手段を含むことを特徴とする知的情報処理方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、文書、図形、画像、データベースなどの情報伝送および処理において、任意の情報の各部分に、誤り訂正符号と暗号化技術とを適用する知的情報処理方法および装置に関する。

【0002】

【従来の技術】 文書、図形、画像、データベースなどの情報伝送および処理において、情報が誤りなく伝送されること、さらに、第三者に盗竊されないことが必要である。前者に対しては誤り訂正符号の技術、後者に対しては暗号化技術が用いられる。情報のセキュリティ対策は重要である。機密の文書、図形、画像、データベースなどの情報伝送および処理において、回線暗号およびファ

5

イルを全文暗号化してから伝送する方法が用いられる。また、コンピュータによつてファイル管理にはパスワードによるアクセス管理が行われており、アクセス権はファイル単位に与えられる。すなわち、ファイルを読み書きする等の操作を行う際、使用者は、まず、パスワードを入力し、それが登録済みであり、対象ファイルの操作権が与えられているかを検査し、検査に合格したときのみ操作が許可される。

【0003】ファイルの暗号はファイル全体を暗号化している。したがって、情報管理者はファイルを管理するためにファイル全体を平文化するので、情報管理者はコンピュータに入力された、あるいは記憶装置に蓄積された全ての情報を知ることができる。また、文書を暗号化して伝送する場合でも、秘書が文書完成してから暗号化するのが普通である。同様に、回線暗号化して伝送する場合でも、操作者は平文を見ることができる。

【0004】なお、回線暗号の場合は、要求/応答単位に暗号化されるが、自由に暗号化部分を指定することは出来ない。また、データコードはフィールド単位に暗号化されるが自由に変更指定が出来ない。もちろん、その単位内での部分的な暗号化は出来ない。これらの暗号管理は安全保護者が行いすべての暗号文にアクセスしている。したがって、暗号鍵を種々用いて、それを利用してアクセス権限を多様にするという発想はまだ生まれていない。特に、文書作成者自身に機密文書・データの最高のアクセス権限を与える、あるいは文書作成者自身のみアクセス権限を与え、安全保護者あるいは情報管理者には暗号文の内容を知らせないで情報管理を行わせることを可能にしたのが本発明の特徴であるが、この発想は新しく情報管理の効率化、柔軟なシステムの実現に有効である。

【0005】ファクシミリにおいては、機密文は別用紙に書いて回線暗号によって暗号化している。これでは連続的処理が行われず、ファイル単位に暗号化と考えられる。また、単語の重要性に応じて誤り訂正符号を変える方法がある。

【0006】

【発明が解決しようとする課題】一般的に文書、図形、画像、データベースなどの情報はその各部ごとに信頼度と機密度の属性を持つと考えることが出来る。例えば、金額は高い信頼度が必要であり、挨拶などの文は信頼度が低くても良い、すなわち、多少の誤りは許容される。また、新製品の発売価格、発売時期などは期間秘密にしておきたい、すなわち、機密度が高いと考えられる。従来の情報伝送および処理においては、これらの情報部分の持つ信頼度と機密度の属性を無視して、一括符号化および暗号化を行ってきた。これでは情報部分の情

報的性質(属性)を生かした知的効率的な情報伝送および処理を行うことができない。処理速度も遅くなる。

【0007】秘書が文書を完成させてから全文を暗号化

6

すると、秘書が機密情報を知ることになる。同様に、回線暗号化においても操作者が平文を見ることができる。

また、ファイル管理において、パスワードでアクセス権を検査する方法および全文暗号化方式では、情報管理者が最高のアクセス権を持っている。そのため、人事情報等の機密情報はコンピュータに入力されないことも多い。したがって、情報の属性を生かした効率的な符号化、暗号化が必要であり、さらに、秘書や回線暗号操作者および情報管理者に機密情報を知られないで情報伝送および処理ができることが望まれる。

【0008】本発明は、かかる問題を解決するためになされたものであって、情報の任意の部分を区分けし、それぞれに信頼度と機密度の属性を設定し、それに応じた誤り訂正符号と暗号化技法を用いた処理を行い、同時に、機密度に対応したファイル内アクセス権を用いることを可能にした知的情報処理方法および装置を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明に係る第1の知的情報処理方法は、文書、図形、画像等の情報伝送および処理において、信頼度レベルとして0からmまでのレベルを用い、また、機密度レベルとして0からnまでのレベルを用いて、CRT等の表示部上で、情報の任意の各部分に、信頼度レベルと機密度レベルの属性を設定し、それぞれに応じた誤り訂正符号と暗号化の技法および暗号鍵を用いて、符号化および暗号化を行い、情報処理および伝送、保存を行う。下記の(1)ないし(6)の手段と、符号化および暗号化されたデータを受信あるいは外部メモリから呼び出し、復号化および平文化を行い情報の処理を行う。下記の(7)ないし(11)の手段とを含むことを特徴とする。

【0010】(1)文書、図形、画像等のデータを作成する手段。

(2)情報の任意の部分を区分けし、その情報各部に信頼度レベルと機密度レベルの属性を設定する手段。

(3)パスワード、暗号鍵のチェックを行う手段。

(4)情報各部をその機密度レベルに応じた暗号化法あるいは暗号鍵を用いて暗号化する手段。

(5)情報各部をその信頼度レベルに応じた誤り訂正符号を用いて符号化する手段。

(6)符号化および暗号化された情報を、伝送あるいは保存等の処理を行う手段。(7)データ、ファイルを受信あるいは外部メモリから呼び出す手段。

(8)パスワード、暗号鍵のチェックを行う手段。

(9)信頼度属性に応じて情報各部を復号化する手段。

(10)機密度属性に応じて情報各部を平文化する手段。

(11)情報処理を行う手段。

【0011】また、本発明に係る第1の知的情報処理装置は、文書、図形、画像等の情報伝送および処理において、信頼度レベルとして0からmまでのレベルを用い、

7

また、機密度レベルとして0からnまでのレベルを用いて、CRT等の表示部上で、情報の任意の各部分に、信頼度レベルと機密度レベルの属性を設定し、それぞれに応じた誤り訂正符号と暗号化の技法および暗号鍵を用いて、符号化および暗号化を行い、情報処理および伝送、保存を行う、下記の(1)ないし(6)の手段と、符号化および暗号化されたデータを受信あるいは外部メモリから呼び出し、復号化および平文化を行い情報の処理を行う、下記の(7)ないし(11)の手段とを含むことを特徴とする。

【0012】(1)文書、図形、画像等のデータを作成する手段。

(2)情報の任意の部分区分けし、その情報各部に信頼度レベルと機密度レベルの属性を設定する手段。

(3)パスワード、暗号鍵のチェックを行う手段。

(4)情報各部をその機密度レベルに応じた暗号化あるいは暗号鍵を用いて暗号化する手段。

(5)情報各部をその信頼度レベルに応じた誤り訂正符号を用いて符号化する手段。

(6)符号化および暗号化された情報を、伝送あるいは保存等の処理を行う手段。(7)データ、ファイルを受信あるいは外部メモリから呼び出す手段。

(8)パスワード、暗号鍵のチェックを行う手段。

(9)信頼度属性に応じて情報各部を復号化する手段。

(10)機密度属性に応じて情報各部を平文化する手段。

(11)情報処理を行う手段。

【0013】また、本発明に係る第2の知的情報処理方法は、機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだままで、平文部分の見出し、キーワード等のファイル管理に必要な情報を直接操作あるいは検索してファイル管理を行う手段とを含むことを特徴とする。また、本発明に係る第2の知的情報処理装置は、機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだままで、平文部分の見出し、キーワード等のファイル管理に必要な情報を直接操作あるいは検索してファイル管理を行う手段とを含むことを特徴とする。

【0014】なお、以下で述べる「Aおよび/またはB」はAのみ、Bのみ、AとBの三者を表すものとする。また、本発明に係る第3の知的情報処理方法は、データベース・システムの任意の、データ項目、レコード(行情報)、データ項目全体(列情報)にその信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化および/または平文化を行う手段とを含むことを特徴とする。

8

【0015】また、本発明に係る第3の知的情報処理装置は、データベース・システムの任意の、データ項目、レコード(行情報)、データ項目全体(列情報)にその信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化および/または平文化を行う手段とを含むことを特徴とする。

【0016】また、本発明に係る第4の知的情報処理方法は、データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分区分けする手段と、その各部分に、信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手段とを含むことを特徴とする。

【0017】また、本発明に係る第4の知的情報処理装置は、データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分区分けする手段と、その各部分に、信頼度レベルおよび/または機密度レベルの属性を設定する手段と、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う手段とを含むことを特徴とする。

【0018】また、本発明に係る第5の知的情報処理方法は、文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0からnまでのレベル(レベル0、1のみを使用する方法を含む)を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにあってはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定し、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化を行う情報処理において、機密度レベルに対応させてアクセス権限レベルを設定し、パスワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する手段を含むことを特徴とする。

【0019】また、本発明に係る第5の知的情報処理装置は、文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0からnまでのレベル(レベル0、1のみを使用する方法を含む)を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにあってはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定し、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化を行う情報処理において、機密度レベルに対応させてアクセス権限レベルを設定し、パ

9

スワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する手段を含むことを特徴とする。

【0020】また、本発明に係る第6の知的情報処理装置は、機密を要するファイルおよびデータを回線暗号化して伝送する際、ファイル管理、暗号化処理に必要な情報部分を平文にしておき、機密を要する部分を暗号化する手段と、そして、暗号文を含んだファイル、データを、さらに、回線暗号化する手段と、それを伝送する手段を含むことを特徴とする。

【0021】また、本発明に係る第7の知的情報処理装置は、ファクシミリを用いて、文書を伝送する際、送信文書にシール添付領域を設けバーコード等のシールをはるか、行カウント機能を利用する等して、行単位あるいはドット単位等に同一ページ内の通常文と機密を要する文を区分する手段と、通常文は普通に伝送し、機密を要する文は暗号化機能に切替えて暗号化して伝送する手段と、受信側では、いったん暗号文を含んだ全文を記憶装置に格納するとともに、通常文のみ印刷出力した後、パスワード、暗号鍵を利用して暗号文の平文化、印刷などの処理を特定者のみに限定する手段とを含むことを特徴とする。

【0022】また、本発明に係る第8の知的情報処理方法は、使用する装置あるいはソフトウェアごとに使用する暗号鍵を登録し、その履歴リストを作成しておき、場合によっては暗号化して保存し、暗号鍵の忘却、紛失の際、その履歴リストを利用して、ファイルあるいはその部分に対して使用した暗号鍵を検索、検証して捜し出す手段を含むことを特徴とする。

【0023】

【作用】本発明の第1の知的情報処理方法、装置においては、文書、図形、画像等の情報伝送および処理において、情報の任意の各部分に、信頼度レベルと機密度レベルの属性を設定すると、パスワード、暗号鍵が登録、検査された後、それぞれに応じた誤り訂正符号と暗号化の技法および暗号鍵を用いて、符号化および暗号化が行われ、情報処理および伝送、保存がなされる。そして、データが受信あるいは外部メモリから呼び出されると、復号化および平文化が行われる。

【0024】また、本発明の第2の知的情報処理方法、装置は、機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分を平文にしておき、機密を要する部分が暗号化され、暗号文を含んだままで、平文部分の見出し、キーワード等のファイル管理に必要な情報が直接操作あるいは検索されて、ファイル管理が行われる。

【0025】また、本発明の第3の知的情報処理方法、装置は、データベース・システムの任意の、データ項目、レコード（行情報）、データ項目全体（列情報）にその信頼度レベルおよび/または機密度レベルの属性を

10

設定すると、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化が行われる。

【0026】また、本発明の第4の知的情報処理方法、装置は、データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分とを区分し、その各部分に、信頼度レベルおよび/または機密度レベルの属性を設定すると、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化が行われる。

【0027】また、本発明の第5の知的情報処理方法、装置は、文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0からnまでのレベル（レベル0、1のみを使用する方法を含む）を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定すると、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化が行われ、機密度レベルに対応させてアクセス権限レベルが設定されているので、パスワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する。

【0028】また、本発明の第6の知的情報処理装置は、機密を要するファイルおよびデータを回線暗号化して伝送する際、ファイル管理、暗号化処理に必要な情報部分を平文にしておき、機密を要する部分のみ暗号化されており、暗号文を含んだファイル、データが、さらに、回線暗号化されて伝送される。

【0029】また、本発明の第7の知的情報処理装置は、ファクシミリを用いて、文書を伝送する際、送信文書にシール添付領域を設けバーコード等のシールをはるか、行カウント機能を利用する等して、行単位あるいはドット単位等に同一ページ内の通常文と機密を要する文が区分され、通常文は普通に伝送され、機密を要する文は暗号化機能に切替えて暗号化して伝送される。受信側では、いったん暗号文を含んだ全文を記憶装置に格納するとともに、通常文のみ印刷出力した後、パスワード、暗号鍵を利用して暗号文の平文化、印刷などの処理を特定者のみに限定する。

【0030】また、本発明の第8の知的情報処理方法は、使用する装置あるいはソフトウェアごとに使用する暗号鍵を登録し、その履歴リストを作成しておき、場合によっては暗号化して保存しているもので、暗号鍵の忘却、紛失の際、その履歴リストを利用して、ファイルあるいはその部分に対して使用した暗号鍵を検索、検証して捜し出す。

【0031】

11

【実施例】以下本発明をその実施例を示す図面に基き詳述する。第1図は第1の発明に係る知的情報処理方法のフローチャート、第2図はその実施に使用する装置のブロック図である。第2図において図示しないキーボード、マス、カメラ等によって文書、図形、画像等のデータが制御部10に入力される。制御部10はマイクロプロセッサからなり、メモリ7に書き込まれている制御プログラムに従ってデータ処理を行う。以下この処理機能を有する仮想的ブロックを想定して説明する。なお、0内の数字は第1図の手順の番号である。データはデータ作成・情報処理手段1によって、作成、加工される(1)。情報各部の区分け・その信頼度・機密性の設定手段2によって、CRT等の表示部8上で、情報の任意の各部分に区分けし、それぞれの部分に、信頼度レベル(0からm)と機密性レベル(0からn)の属性を設定する(2)。そして、データ作成・情報処理手段1によってパスワード、暗号鍵の登録および検査を行う(3)。つまり、まず、暗号化手段3によって、各部をその機密性レベルに応じた暗号化の技法および暗号鍵を用いて、暗号化を行う(4)。そして、符号化手段3によって、各部をその信頼度レベルに応じた誤り訂正符号を用いて符号化する(5)。そして、データ作成・情報処理手段1によって、伝送および保存を行う(6)。さて、受信側等では、データ作成・情報処理手段1によって、データおよびファイルなどの情報を受信あるいは補助メモリ(外部メモリ)9から呼び出し(7)、ついで、パスワード、暗号鍵の検査を行う(8)。検査に合格すれば、復号化手段5によって、信頼度レベルに応じた誤り訂正符号によって復号化する(9)。そして、平文化手段6によって、機密性レベルに応じた暗号化の技法および暗号鍵を用いて、平文化を行う(10)。さらに、必要があればデータ作成・情報処理手段1によって情報処理をする(11)。

【0032】さて、第3図に画面上での情報属性の設定例を示す。情報各部の区分けのために、区切り記号として、 π [] π などを用いているが、この間で挟まれた部分は、機密性レベル1、信頼度レベル0である。第4図には設定された情報属性表である。図形、画像等は区切り記号を使用するのは好ましくないため、マウスなどで2点の座標を指定し、それを対角線とする長方形の情報属性を設定して、暗号化、暗号化などに際しては、この情報属性表を使用する。なお、信頼度レベルが0のときは情報はそのままである。レベルの数字が高いほど誤りは許されないで、符号化による長い検査ビットが付加される。また、機密性レベルが0のときは情報は平文のままである。レベルの数字が高いほど情報の盗聴、漏洩は許されないでより複雑な暗号を使用する。しかし、確実な暗号を一種類用いて、暗号鍵のみ異なるものを使用する場合もあるが、これはファイル内アクセスを用いる場合であり後述する。

【0033】なお、第1図のフローチャートの手順は必

12

ずしもこの順序通りでなくとも良い。色々のバリエーションがあるが省略する。さて、第1の本発明に係る知的情報処理方法および装置では、信頼度と機密性の両方を用いた。これは暗号文の1ビットエラーは平文化するときビットのエラーとなる。つまり、エラーに弱い傾向があるので、暗号と誤り訂正符号を併用する利点がある。もちろん、どちらか一方のみを使用するシステムも可能である。これについては第1の本発明に係る知的情報処理方法および装置で信頼度と機密性のどちらか使用しない方を省けば良い。

【0034】第1の発明の知的情報処理方法、装置の直接的効果は効率的符号化および暗号化と処理速度の向上であるが、そのほかにも下記に示す種々の効果がある。第5図は、第2の発明に係る知的情報処理方法、装置に使用するファイル例である。機密を要するファイルをディスク等に保存して管理を行う際、見出しおよびファイル管理に必要な情報部分1を平文(部分暗号にしてもよい)にしておき、機密を要する本文2を暗号化(部分暗号にしてもよい)する。そして、暗号文を含んだままで、平文部分の見出し、キーワード等のファイル管理に必要な情報を直接操作あるいは検索してファイル管理を行う。これによって、ファイル管理が容易となり効率が向上すると共に、情報管理者に暗号文の内容を知られないようにすることもできる。

【0035】なお、以下で述べる「Aおよび/またはB」はAのみ、Bのみ、AとBの三者を表すものとする。第6図は第3の発明に係る知的情報処理方法のフローチャートであり、一例として、任意の項目を暗号化および符号化して登録する例である。一般には、データベース・システムの任意の、データ項目、レコード(作情報)、データ項目全体(列情報)にその信頼度レベルおよび/または機密性レベルの属性を設定し、それぞれに応じた誤り訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う。検索、平文化およびレコード、データ項目全体に対する処理も同様である。

【0036】また、第3の発明に係る知的情報処理装置は、第1の発明のデータ作成・情報処理手段1にデータベース処理機能を持たせれば、第2図と同様である。さて、第7図は関係データベースの情報属性の設定例である。(a)はデータ項目ごと、(b)はレコード全体、(c)はデータ項目全体に情報属性を設定する場合である。第8図は1レコード/画面の属性設定例である。任意の項目に属性を設定すると同時に、画面右上の信頼度・暗号属性設定欄を用いて、レコード全体の属性を一括設定する。

【0037】第4の発明に係る知的情報処理方法、装置は、データベースの項目を一つのファイルとして捉え、項目内の情報の任意の部分に区分けし、その各部分に、信頼度レベルおよび/または機密性レベルの属性を設定

13

す。そして、それぞれに応じた誤訂正符号および/または暗号化の技法および暗号鍵を用いて、符号化および/または暗号化、復号化および/または平文化を行う。この発明は、第1と第3の発明から構成されるので詳細は省略する。

【0038】第9図は第5の発明に係る知的情報処理方法、装置のファイル内およびデータベース内のアクセス権限レベルを示す。この発明では、文書、図形、画像、データベース等の情報伝送および処理において、機密度レベルとして0からnまでのレベル(レベル0、1のみ) 10 を使用する方法を含む)を用いて、CRT等の表示部上で、情報の任意の各部分に、特に、データベースにあってはデータベースの任意の項目、任意のレコード、任意のデータ項目全体あるいは項目内の情報の任意の部分に、機密度レベルの属性を設定し、それぞれに応じた暗号化の技法および暗号鍵を用いて、暗号化および平文化を行う。そして、機密度レベルに対応させてアクセス権限レベルを設定し、パスワードや暗号鍵を利用して、その情報部分のアクセスをそのレベルに従って複数の特定者に限定する。すなわち、従来ファイル単位に与えられていたアクセス権限をファイル内に持込み、ファイル内 20 アクセス権限を設定するという新しい概念を用いている。

【0039】例えば、機密度レベル0、1、2、3を使用している時、その対応する部分をアクセスする権限は、それぞれアクセス権限0、1、2、3である。したがって、社長はアクセス権限0、1、2、3を持ち、レベル1、2、3の暗号鍵を所有する。重役はアクセス権限0、1、2を持ち、レベル1、2の暗号鍵を所有するようにする。レベル0は平文で誰でも読むことができる。また、パスワードを併用しても良い。そして、部分的な暗号化なので、暗号文はそのままでファイル管理が行えるので、情報管理者に全てのアクセス権限を与えないで情報管理が可能となる。したがって、文書作成者あるいは社長が最高のアクセス権限を持つことが可能となる。安全保護者を置くにしてもアクセス権限を限定できる。

【0040】なお、この発明の方法、装置は第1、2、3、4の発明から構成されるので詳細を省略する。次に、この発明の最も簡単な実施例として、部分暗号化による文書処理システムの送信部のフローチャートを第10図、受信部のフローチャートを第11図に示す。第12図はその画面上の動作例である。ここでは、誤訂正符号は使用しないとする。したがって、信頼度レベルは0のみである。また、機密度レベルは0と1、したがって、アクセス権限レベルも0と1とする。説明を分かり易くするため、文書処理システムの操作者は社長と秘書とする。秘書にはアクセス権限レベル0を割り当て通常文のみ処理を許可する。社長にはアクセス権限レベル1を割り当て、通常文と暗号文の処理を許可する。ここで 50

14

は、暗号化/平文化ツールは暗号化および平文化機能を持つソフトプログラムであり、通常の文書処理システムにこのプログラムが付加されているものとする。以下に操作例を述べる。

【0041】まず、秘書がワープロ等で平文の作成を第12図の画面1上で行う(1)。いったん補助記憶装置に保存しても画面に表示したままでもよいが、次に社長と操作を交替する。社長は機密文を通常文で入力する。画面1に示すように、この文を特殊記号# [] まで挟む。そして、いったん保存する(2)。次に暗号化ソフトを起動し、社長のみが知っているパスワード、暗号鍵を入力する(3)。そして、先ほど保存した文書ファイルと呼び出して暗号化を実行する(4)。実行すると、そのま 20 ま暗号化しても良いが、ここでは、まず# [] まで挟まれた機密文を空文にするか、第12図の画面2のように特殊記号[]に変換する(5)。ついで暗号化を実行する。バイナリモードの暗号文が得られるが、汎用性を考慮して、16進アスキーコードに変換して第12図の画面2に示すように、文末の##記号の後に順次付加する(6)。バイナリモード使用可能な文書処理および通信ソフトを使用する場合は、汎用化のためのこの変換は必要ない。暗号化を終了すると、暗号文の末尾に##記号を付加し補助記憶装置に保存され、通常文ファイルは削除される(7)。文書ファイルを伝送する場合は、秘書が通信ソフトを起動して暗号文ファイルを伝送する(8)。

【0042】次に、平文化処理について述べる。ディスク、ハードディスクなどの補助記憶装置で情報を受け取るか、受信した場合は、秘書がワープロ等で平文の部分を確認する。オンラインで直接受信して画面表示している場合は平文の部分を確認後、いったん補助記憶装置に保存する(9)。次に社長は暗号化ソフトを起動させてパスワードを入力し、平文化処理を選択し、暗号鍵を入力する(10)。そして暗号文ファイルと呼び出して平文化を実行する(11)。##の後の16進アスキーコードの暗号文をバイナリモードに変換して(12)、さらに平文化した平文を、# [] まで挟まれた特殊記号[]の箇所へ挿入する(13)。平文化処理が終了と第12図の画面1の状態に戻る。いったん保存し、ワープロ等を起動して編集、印刷等の処理をした後、必要なら通常文ファイル 40 を削除する(14)。以上の操作で、社長は機密データを秘書に知られることなく文書処理および通信を実行できる。

【0043】なお、暗号化/平文化処理をワープロ等に組み込んでおけば、文書ファイルをいちいち保存することなく画面表示したまま処理を続けられるが、原理は上記で述べたものと同じである。また、本方式は電子メール、電子キャビネット、データベースなどのシステムあるいは個人のファイル管理に直接適用できる。また、暗号文を含んだメールを電子掲示板に表示させ、暗号鍵

15

を所有しているグループのみが復元して平文を得ることもできる。第6の発明に係る知的情報処理装置においては、機密を要するファイルおよびデータを回線暗号化して伝送する際、ファイル管理、暗号化処理に必要な情報部分は平文のまま、機密を要する部分はまもって直接の担当者が暗号化しておく。そして、暗号文を含んだファイル、データを、暗号操作者によって回線暗号化して伝送する。これによって、暗号操作者に機密情報を知られることがなくなる。このためには、回線暗号装置のほかに、第1の発明の装置を用いれば良い。

【0044】第13図は第7の発明に係る知的情報処理装置（ファクシミリ部分暗号化装置）の原理図である。まず、送信側では送信用紙1を作成する。そして、シール添付領域にバーコード等のメッセージシールを貼り付ける。第13図で「S」は文書の先頭、「E」は文末を意味する。つまり、「S」は機密文ブロックの初め、「T」は機密文ブロックの終わりを意味する。ここでは行単位に機密文エリアを設定する。そして、例えば、ファクシミリの数字ボタンによって機密文を含んでいることを入力し、ついで文書番号を入力して、送信ボタンを押して送信する。平文はそのまま、機密文は暗号化されて送信される。

【0045】受信側では暗号文を含んだ文書を受信すると、受信用紙2に通常文のみ印刷し、暗号文の箇所には暗号文の所在を知らせるマーク@を印刷しておく。同時に暗号文を含んだ全文を補助メモリ3に記憶しておく。秘書は通常文を確認し社長に連絡する。社長はファクシミリにパスワード、暗号鍵、文書番号を入力し、ファクシミリの暗号機能を用いて平文化処理をして平文を印刷する。以上の操作では、送信側では情報を秘書に知られるが、受信側では機密文は社長だけが知り得る。

【0046】第8の発明に係る知的情報処理方法は、使用する装置あるいはソフトウェアごとに使用する暗号鍵を登録し、その履歴リストを作成しておき、場合によっては暗号化して保存し、暗号鍵の忘却、紛失の際、その履歴リストを利用して、ファイルあるいはその部分に対して使用した暗号鍵を検索、検証して捜し出す。

【0047】

【発明の効果】以上のように本発明によれば、以下の効果がある。

- (1) ファイル内あるいは伝送される情報の各部分の信頼度、機密度に応じた信頼度レベル、機密度レベルを設定し、それぞれに応じた誤り訂正符号、暗号化手法を用いることにより、効率的な符号化、暗号化を可能とした。
- (2) 部分的暗号化、符号化によって、全文暗号化、符号化より、情報処理速度が向上する。
- (3) 機密度レベルに対応したファイル内あるいは伝送情報内のアクセス権限レベルを設定し、パスワード、暗号鍵を特定者にもみ使用させることにより、機密情報のアクセスを特定者に限定することを可能とした。

16

(4) ファイルに平文と暗号文の混在を許容し、ファイル管理情報を平文で付加し、機密部分のみは暗号文のまま操作できることで効率的なファイル管理が実現可能となった。

(5) 機密情報のアクセス権限を文書作成者（社長も可能）あるいは業務上の直接的責任者に限定でき、情報管理者に最高のアクセス権限を与えないことが可能である。たとえば、秘書に平文を書かせ、社長は秘書に知られないで機密文をその文書に挿入できる。

(6) 暗号鍵の履歴リストを用いて、暗号鍵の誤使用、紛失等を防ぐことができる。

(7) 柔軟なセキュリティ管理システムが構築できる。

(8) 柔軟な電子文書システムが構築できる。

本発明は大型機にも適用できるが、セキュリティ確立の困難なネットワーク、ワークステーション、パーソナルコンピュータには特に有効である。

【図面の簡単な説明】

【図1】第1の発明の知的情報処理方法のフローチャートである。

【図2】第1の発明の実施に使用する装置のブロック図である。

【図3】画面上での情報属性の設定例である。

【図4】設定された情報属性表である。

【図5】第2の発明の知的情報処理方法、装置に使用するファイル例である。

【図6】第3の発明の知的情報処理方法のフローチャートである。

【図7】関係データベースの情報属性の設定例である。

【図8】1レコード／画面の属性設定例である。

【図9】第5の発明のファイル内およびデータベース内のアクセス権限レベルである。

【図10】部分暗号化による文書処理システムの送信部のフローチャートである。

【図11】部分暗号化による文書処理システムの受信部のフローチャートである。

【図12】部分暗号化による文書処理システムの画面上の動作例

【図13】第7の発明のファクシミリ部分暗号化装置の原理図である。

【符号の説明】

【図2】1 データ作成・情報処理手段

2 情報各部の区分け・その信頼度・機密度の設定手段

3 暗号化手段

4 符号化手段

5 復号化手段

6 平文化手段

7 メモリ

8 CRT表示部

50 9 補助メモリ

10 マイクロプロセッサ

2 暗号文画面

【図5】1 見出し部およびファイル管理部

【図13】1 送信用紙

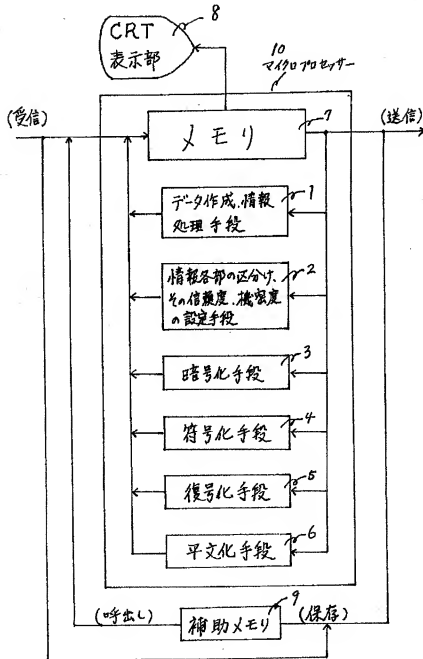
2 データ本体

2 受信用紙

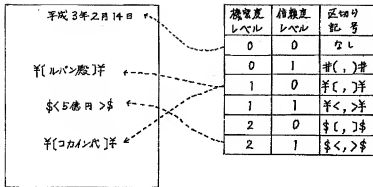
【図12】1 平文画面

3 補助メモリ

【図2】



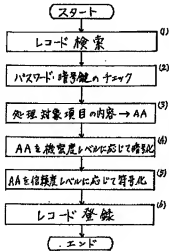
【図3】



【図4】

情報部分	信頼度レベル	機密度レベル
(100, 200) (300, 250)	0	1
(100, 300) (200, 350)	3	3
(100, 400) (250, 500)	1	2
⋮	⋮	⋮
⋮	⋮	⋮

【図6】



【図8】

氏名 _____

年齢 _____

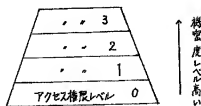
所属 _____

業績査定

☆☆ _____

属性設定

【図9】



【図5】

1

ファイル名、見出し
キーワード、-----
(ファイル管理情報：部分暗号可)

2

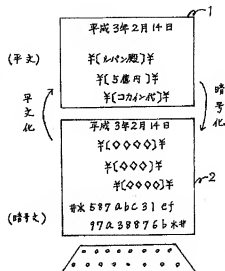
(データ本体)

部分暗号
あるいは
全文暗号

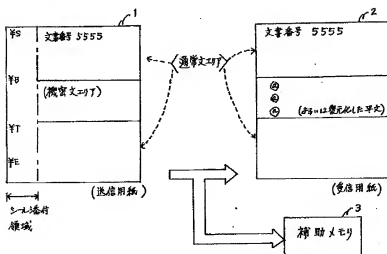
【図7】



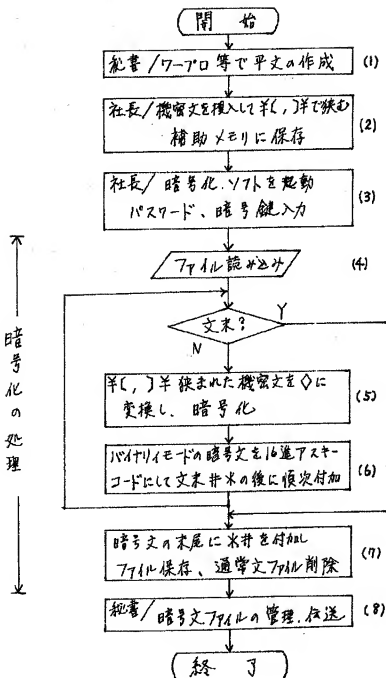
【図12】



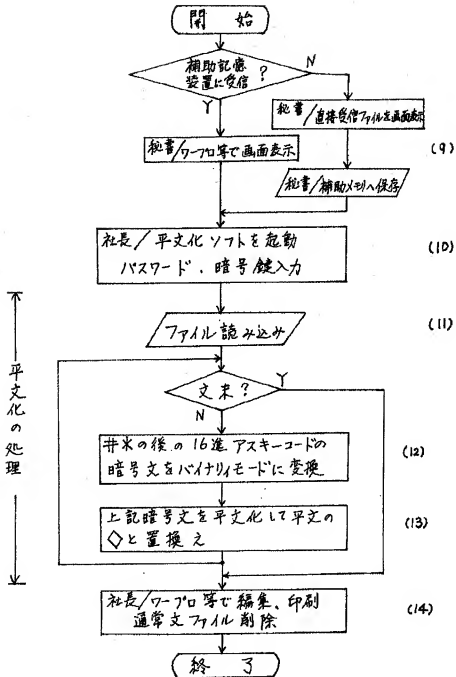
【図13】



【図10】

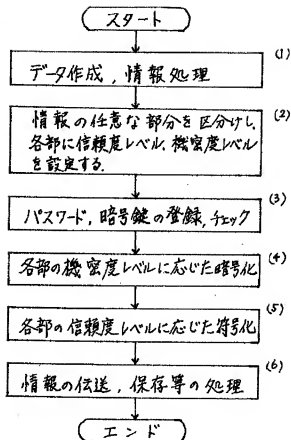


【図11】



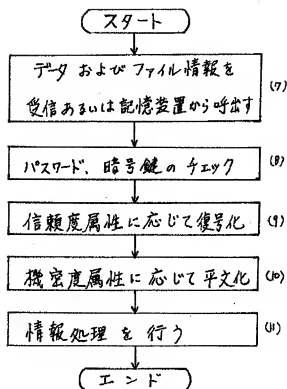
【図1】

(a)



【図1】

(b)



【手続補正書】

【提出日】平成5年2月19日

【手続補正3】

【補正対象書類名】図面

【補正対象項目名】全図

【補正方法】変更

【補正内容】

【図4】

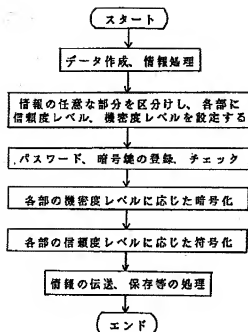
情報部分	信頼度レベル	機密度レベル
(100, 200) (300, 250)	0	1
(100, 300) (200, 350)	3	3
(100, 400) (250, 500)	1	2
・	・	・
・	・	・
・	・	・

【図9】

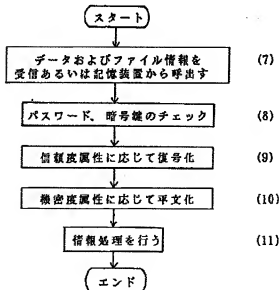


【図1】

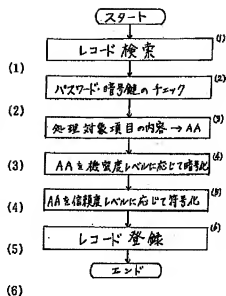
(a)



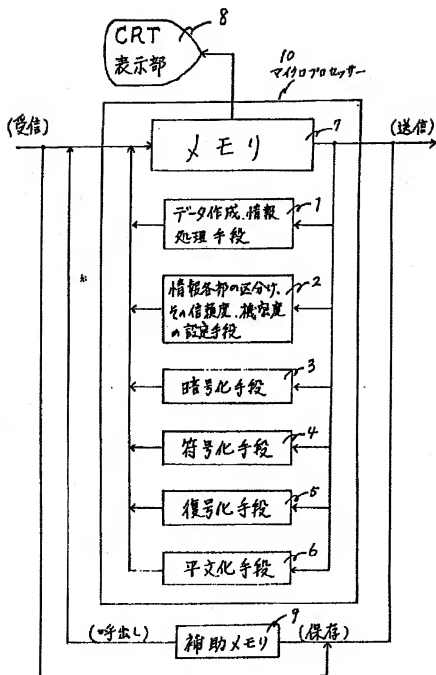
(b)



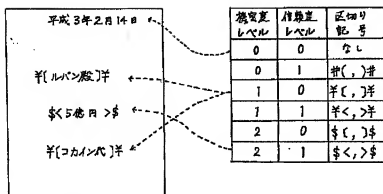
【図6】



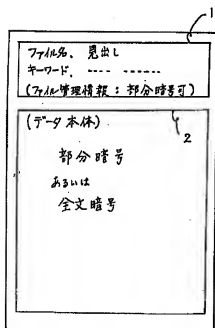
【図2】



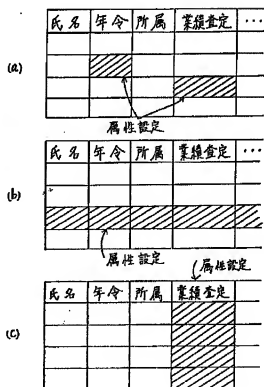
【図3】



【図5】



【図7】




【図8】

氏名 _____

年齢 _____

所属 _____

属性設定 

☆☆ _____

住所 暗号
(コード全体)

属性設定

【図12】

(平文)

平成3年2月14日

¥(ルパン殿)¥

¥(5店円)¥

¥(コカ12代)¥

暗号化

平成3年2月14日

¥(◇◇◇◇)¥

¥(◇◇◇)¥

¥(◇◇◇◇)¥

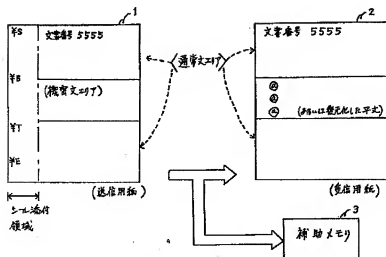
暗号文

※58746C31Cf

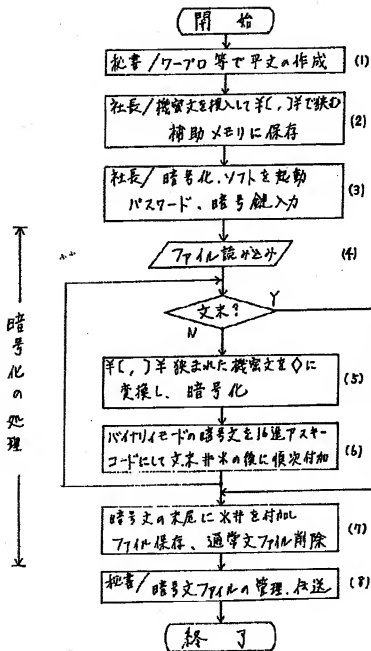
97A388766b※

早文化

【図13】



【図10】



【図11】

